Introduction

Today's information security challenges are greater than ever. Systems are more complex and interconnected than ever before. Viruses, hackers, and disgruntled employees can bring information systems to a halt; intruders can compromise or alter data. INFOSEC engineering provides a systems solution for protecting your data during processing, transmission, and storage. **NISE East Defensive Information Warfare Engineering Division** personnel are capable and ready to assist you in **ALL** areas where information resources are critical.

Contact us TODAY and let us show you how we can provide you with the right INFOSEC solution.

Please send all correspondence to:

Commanding Officer
Code 72
Naval Command, Control and Ocean Surveillance Center, In-Service Engineering, East Coast Division (NISE East)
P.O. Box 190022
North Charleston, SC 29419-9022

INFOSEC Services

NISE East INFOSEC Help Desk

COML: (800) 304-INFOSEC (4636)
DSN: 563-8878 or 563-8879
E-mail: ***infosechd@niseeast.nosc.mil***

INFOSEC Servers

WWW Server: The One Stop Shop for Naval INFOSEC Products and Services,
URL: ***http://infosec.nosc.mil/infosec.html***

FTP Server: ***ftp://infosec.nosc.mil***.
Registered Military Domain access only.

Naval Electronic Bulletin Board System (NEBBS): (800) 494-9947 or (803) 974-4495
DSN: 563-8880
28800 bps with 8/N/1 modem settings.

INFOSEC/COMPUSEC Advisory E-mail List:
majordomo@sprocket.nosc.mil.
Place "Subscribe csa" in the body of your message. No subject line please. New advisories will be
e-mailed to you automatically.

The Naval Computer Incident Response Team (NAVCIRT), located at the Fleet Information Warfare Center (FIWC). **(800) 628-8893**, (804) 464-8832 or 24-hour Voice Mail pager (800) 759-7243, PIN 5294117

U.S. NAVY INFOSEC Tools, Tips & Services

Information Warfare-Protect Systems Engineering Division

1-800-304-INFOSEC (4636)

infosechd@niseeast.nosc.mil

http://infosec.nosc.mil/infosec.html

Top UNIX Security Tips

Patches: Install the latest security-relevant software patches for your programs such as sendmail, rdist, loadmodule, and syslogd.

Sendmail: Disallow mailing directly to programs. Use current release with current patches.

rdist: Ensure current release does not have race condition that can be exploited to gain root access.

Loadmodule: Latest release patches security hole that allows root access.

syslogd: Current release addresses race condition vulnerabilities.

Default logins: Eliminate default account/password combinations.

Passwords: Use passwords not found in any dictionary. Most password crackers use dictionary-based attacks. Try using the first or second letter of an eight word phrase.

Different Passwords: Accounts on different hosts should have different passwords to minimize risk of multiple host penetrations.

.rhosts & hosts.equiv files: Restrict or eliminate non-administrative use.

Auditing: Turn on auditing to establish accountability for user actions, troubleshooting, and damage control.

Secure NFS: Get latest patches and do not allow fileserver to export to itself or to the world. If possible, disable NFS.

AIX rlogin: Get patched version which disallows unauthorized access to password accounts.

tftp: Disable tftp and any other services you don't require.

Detailed descriptions are available at:
ftp://infosec.nosc.mil/pub/docs/unix/quickfix.txt

Top UNIX Security Tools

ICE-PICK: Internet domain scanner used to identify host vulnerabilities, developed by NRL.

Computer Oracle and Password Systems (COPS): System configuration inspection and analysis tool which targets known weaknesses.

Security Profile Inspector (SPI): System-specific configuration/password assessment tool.

SOCKS: Set of tools to provide selective secure network access through a firewall.

TCP Wrappers: Monitors/filters incoming network traffic.

Tripwire: Monitors a designated set of files for any alterations.

npasswd/passwd+/shadow: Replacements for existing password programs that eliminate the choosing of poor passwords.

Crack: High speed. dictionary-based password cracking tool.

TAMU Tools: TIGER system security checker, Drawbridge packet filter.

Licensed DoD AntiViral Software

IBM AntiViral Software version 2.5

Available at:
ftp://infosec.nosc.mil/pub/tools/dos/virus/IBM/

NORMAN Anti-Viral Software version 3.50

Available at: **ftp://infosec.nosc.mil/pub/tools/dos/virus/NORMAN-ANTIVIRUS/**

Top Windows NT Security Tips

Default logins: Disable guest account/password combinations.

Administration: Rename the Administrator account. An intruder now has to guess that name if they want total control.

Registry Values: Make the HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES tree read-only.

Permissions: Reset permissions on the TEMP directory (C:\TEMP) to full control for SYSTEM, ADMIN, CREATOR. Everyone or users should have add permission only.

Passwords: Use passwords not found in any dictionary. Most password crackers use dictionary-based attacks. Try using the first or second letter of an eight word phrase.

Auditing: Turn on auditing to establish accountability for user actions, troubleshooting, and damage control. In the User Manager, select all failure events, successful Logon and Logoff, User and Group Management, Security Policy Changes, and Restarts.

User Rights: Backup/Restore user rights allow reading/writing of all files. Make sure you are auditing the use of Backup/Restore rights.

C2 Configuration Manager: Obtain the Windows NT Resource Kit and install it. Windows NT is C2 compliant and this utility will help you set the system up for C2 compliance.

Windows 95 Security Tip

Password Encryption: The mechanism used to protect the Windows 95 password cache is weak and easily broken. Get the Microsoft security update to correct this problem. The security enhancement increases the encryption key from 32 to 128 bits, significantly improving the protection of the password cache file. The security update is available at the Microsoft WWW site (www.microsoft.com).